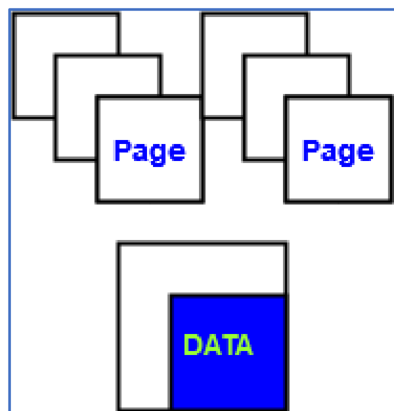
SQLITE DATABASE FORENSICS NOTE

AUNG ZAW MYO
Digital Forensics Myanmar

SQLite ကို Android Phone, Apple Phone, MAC OS, Window တို့မှာ အချို့ Application တွေရဲ့ Data တွေကို သိမ်းဆည်းဖို့ အများဆုံးအသုံးပြုပါတယ်။ Message Application တွေဖြစ်တဲ့ Viber, Telegram, What App , Skype, Messenger စတဲ့ Message Application တွေက Desktop Version ပဲဖြစ်ဖြစ် Mobile Version ပဲ ဖြစ်ဖြစ် SQLite Database ကို အသုံးပြုပါတယ်။

ဒါ့အပြင် Contact, Call Log , Message (SMS) စတာတွေမှာ SQLite Database ကို အသုံးပြုပါတယ်။ Window ဆိုရင်လဲ Browser တွေရဲ့ History , Window Timeline History ကိုသိမ်းဆည်းတဲ့နေရာ Mac OS ဆိုရင်လဲ အဓိကကျတဲ့ Artifacts တွေကို သိမ်းဆည်းတဲ့နေရာမှာအများဆုံးအသုံးပြုပါတယ်။



SQLite မှာ Journal File 2 File ရှိပါတယ်။

- Journal File
- Write-Ahead Log (WAL) File

Journal File

Database မှာ ရှိတဲ့ Data တွေကို Page အနေနဲ့ သိမ်းထားပြီး Page Size ကတော့ Developer သတ်မှတ်တဲ့ အတိုင်းရှိပါတယ်။ Default ကတော့ 4096 Bytes ဖြစ်ပါတယ်။ Database တစ်ခုထဲမှာ ရှိတဲ့ Page File တွေက Same Size ဖြစ်ပါတယ်။ Page-1 က 4096 Bytes ဆိုရင် ကျန်တဲ့ Page တွေကလဲ 4096 Bytes ပဲဖြစ်ပါတယ်။ Database ထဲမှာ Page-1 Page-2 Page-3 ဆိုပြီး Page file 3 ခုရှိတယ်ဆိုပါတော့။

Page 1 မှာ Data ထည့်မယ်ဆိုရင် Page 1 ထဲမှာ အရင်ကရှိတဲ့ Data က Rollback Journal File အဖြစ်သွားသိမ်းပါတယ်။

Page 1 ထဲကို Data ရောက်ပြီး Commit (Save) လုပ်ပြီဆိုတဲ့ အချိန်ကျရင် Rollback Journal File က မရှိတော့ပါဘူး။ ကြားထဲမှာ Commit (Save) မလုပ်ဘူးဆိုရင် Database Error တစ်ခုခုဖြစ်မယ်ဆိုရင် Journal File ကရှိနေအုံးမှာ ဖြစ်ပါတယ်။ နောက်တစ်ခါ Database ပြန်ဖွင့်ရင် Rollback Journal File ကနေ Error Recovery လုပ်ဖို့ ဖြစ်ပါတယ်။ So, Journal File က SQLite Forensics အတွက်အရေးပါလာပါတယ်။

messages (40)
messages_calls (4)
messages_likes (0)
messages_reminders (0)
participants (4)
participants_info (9)
public_accounts (1)
purchase (0)
recent_searches (0)
recent_stickers (0)
remote_banners (0)
sqlite_sequence (11)
stickers (426)
stickers_packages (8)
Unallocated space (12)

☐		3	2	57780776207042950	1669658831302	57780776207042950	0
☐		2	2	57780775016947122	1669658802852	57780775016947122	0
☐		30	2	57780853857111638	1669660682578	57780853857111638	0
☐		29	2	57780853820872850	1669660681681	57780853820872850	0
☐	Journal	4	2	57780776417970484	1669658836213	57780776417970484	0
☐	Journal	3	2	57780776207042950	1669658831302	57780776207042950	0
☐	Journal	2	2	57780775016947122	1669658802852	57780775016947122	0
☐	Journal	6	2	57780822794855204	1669659942073	57780822794855204	0
☐	Journal	5	2	57780814735034683	1669659749813	57780814735034683	0
☐	Journal	12	2	57780828598509636	1669660080225	57780828598509636	0
☐	Journal	11	2	57780827180041974	1669660046598	57780827180041974	0
☐	Journal	10	2	57780826929176647	1669660040187	57780826929176647	0
☐	Journal	9	2	57780825862565135	1669660015150	57780825862565135	0
☐	Journal	8	2	57780824820196706	1669659990278	57780824820196706	0
☐	Journal	7	2	57780824467627522	1669659981950	57780824467627522	0

Journal File

Write-Ahead Log (WAL) File

သူက Rollback Journal File နဲ့ပြောင်းပြန်ပါ။ အသစ် Write လုပ်မဲ့ Data က WAL File အဖြစ်သွားသိမ်းပါတယ်။ Page-1 မှာ Data ကို Write လုပ်မယ်ဆိုရင် Page-1 ထဲမှာ အရင်ကရှိတဲ့ Data ကို မဖျက်ပဲ ။ အသစ် Write လုပ်မဲ့ Data က WAL File ထဲမှာသွားသိမ်းပါတယ်။ Commit (Save) လုပ်တဲ့ အချိန်ကျမှ Page-1 ထဲကို Data သွားသိမ်းပါတယ်။ Commit (Save) မလုပ်ရင် Database Error တစ်ခုခုဖြစ်ရင် WAL File ထဲမှာ Data တွေကျန်နေပါတယ်။ So, WAL File မှာ New Write လုပ်မဲ့ Data တွေ။ အရင် Data အဟောင်းတွေပါ ရှိနေတတ်တဲ့ အတွက် SQLite Forensics အတွက် အရေးပါတဲ့ File တစ်ခုဖြစ်ပါတယ်။ WAL File ကို နောက်ပိုင်း SQLite Database သုံးတဲ့ Application တော်တော်များများမှာ တွေ့ရပါတယ်။ Read Write ကို တစ်ပြိုင်တည်း လုပ်လို့ရတာ ကြောင့်ဖြစ်ပါတယ်။

Journal, Write-Ahead Log (WAL) File တွေမှာ Commit (Save) မလုပ်ရသေးတဲ့ Recently Added Data ဒါမှမဟုတ် Recently Deleted Data တွေရှိနိုင်ပါတယ်။

Data Structure

Record type	_id [P	chat_	from_	key_ic	sende	status	broad	recipi	particip	origin	origin	tir	receiv	receip	messa	text_data
Wal	21	4	1	B1A9.	0	13	0	0		0	0	8/12/		8/12/	0	Design
Wal	20	4	1	C78A	0	13	0	0		0	0	8/12/		8/12/	0	And you?
Wal	19	4	0	856D	0	0	0	0		0	0	8/12/	8/12/		0	What do you do at wo
Wal	18	4	1	0BC8	0	13	0	0		0	0	8/12/		8/12/	0	Interesting story abou
Wal	17	4	0	4AD2	0	0	0	0		0	0	8/12/	8/12/		0	My day begins with to
Wal	16	4	0	5EAC	0	0	0	0		0	0	8/12/	8/12/		0	Watch movies, TV seri
Wal	15	4	0	15F75	0	0	0	0		0	0	8/12/	8/12/		0	I like to go out with m
Wal	14	4	1	AF19	0	13	0	0		0	0	8/12/		8/12/	0	How does your day be
Wal	13	4	1	795E	0	13	0	0		0	0	8/12/		8/12/	0	What are your custom
Wal	12	4	1	2C90	0	13	0	0		0	0	8/12/		8/12/	0	Tell about your life
Wal	11	4	1	5340	0	13	0	0		0	0	8/12/		8/12/	0	Hi
Wal	10	4	0	4847	0	0	0	0		0	0	8/12/	8/12/		0	Hello
Wal	9	4	1	D31C	0	6	0	0		0	0	8/12/			7	
Wal	8	2	1	2513	0	13	0	0		0	0	1/27/		1/27/	0	Uh

Write-Ahead Log (WAL) File

SQLite Free List Pages

Database ထဲမှာ Active ဖြစ်နေတဲ့ Database File တွေရှိသလို Active မဖြစ်တဲ့ တစ်နည်းအားဖြင့် Data Write မလုပ်ရသေးတဲ့ Page တွေလဲရှိပါတယ်။SQLite Database ထဲကနေ အချို့အချက်အလက်တွေကို Delete လုပ်လိုက်တဲ့အခါမှာ Data အဖျက်ခံလိုက်ရတဲ့ Page တွေက Free List Page ဖြစ်သွားပါတယ်။ နောက်တစ်ကြိမ်မှာ Data Write မယ်ဆိုရင် Free List ဖြစ်နေတဲ့ Page တွေမှာ Data ကို Write လုပ်မှာဖြစ်ပါတယ်။ ဒါကြောင့် SQLite Database ကနေ Data ကို Delete လုပ်လိုက်ရင် ချက်ချင်းပျက်မသွားနိုင်ပါဘူး။ **Free List Pages တွေမှာ Recently Deleted လုပ်ထားတဲ့ Data တွေရှိနိုင်ပါတယ်။** Page က Free List အဖြစ်ရှိနေပါတယ်။ But မသုံးပဲရှိနေတဲ့ Page တွေ။ Data Delete လုပ်တာခံလိုက်ရတဲ့ Page တွေကို Free List အဖြစ်ထားမထားကလဲ Developer နဲ့ Vendor ပေါ်မှာ မူတည်ပါတယ်။

Properties
Tables
Accounts (1)
Alerts (0)
CallMembers (3)
Calls (3)
ChatMembers (10)
Chats (5)
ContactGroups (12)
Contacts (3)
Conversations (9)
DbMeta (4)
LegacyMessages (0)
Messages (53)
Participants (18)
SMSes (0)
Transfers (0)
Voicemails (0)
Unallocated space (0)

Data | Structure

	Record type	id [Pri	is_per	chatn	timestamp	author	from_dispname	chatmr	identities	leaver	body_xml
☐	Freelist	140	1	#belk	2/22/2010 !	+79052045315	+79052045315	18			<partlist alt="">
☐	Freelist	138	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	18			<partlist alt="">
☐	Freelist	103	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	18	belkasofttest3		<partlist alt="">
☐	Freelist	101	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Well, you'll wait a blame
☐	Freelist	99	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Well, go 'long -- who&ap
☐	Freelist	97	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			I won't! You can all go, if
☐	Freelist	95	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Nobody wants you to. Go &ap
☐	Freelist	94	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Who cares!
☐	Freelist	91	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Well, we'll let the cry-bab
☐	Freelist	89	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Oh, shucks! Baby! You want to
☐	Freelist	87	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			But, Joe, there ain't such
☐	Freelist	85	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Just think of the fishing that&a
☐	Freelist	84	1	#belk	2/22/2010 !	belkasofttest	BelkaSoftTest	3			Oh no, Joe, you'll feel be

SQLite Free List Pages

Unlocated Space

Hard Disk မှာရှိတဲ့ Unlocated Space လိုပါပဲ။ But , Unlocated Space ထဲမှာ ရှိတဲ့ Database File တွေမှာ Database Pointer , Database Table တွေကို မရှိတော့တဲ့ အတွက် Recovery လုပ်ဖို့ အချိန်ယူရပါတယ်။ Unlocated ထဲမှာ Raw Data အဖြစ်သာရှိပါတယ်။ Recovery အတွက် Carving ပြန်လုပ်ရပါတယ်။**Unallocated Space မှာတော့ Free List Page တွေထဲမှာ မရှိတဲ့ Deleted Data တွေရှိနိုင်ပါတယ်။**

Properties
Tables
history_client_versions (0)
history_event_listeners (0)
history_events (0)
history_items (12)
history_items_to_tags (2)
history_tags (2)
history_tombstones (0)
history_visits (13)
metadata (1)
sqlite_sequence (2)
Unallocated space (12)

Carved data | Raw data

	URL	Offset (bytes)	Length (bytes)	Origin path
☐	https://www.bbc.com/sport/football/51212537/c	10268	202	
☐	https://www.bbc.com/sport/football/51115604?	10316	154	
☐	https://www.bbc.com/sport0e	10364	106	
☐	https://www.bbc.com/news/world-asia-51221029=	10394	76	
☐	https://www.bbc.com/newsW	10443	27	
☐	https://www.bbc.com/future/article/20200108-the-n	10473	108	
☐	https://www.bbc.com/	10560	21	
☐	https://www.bbc.co.uk/iplayer/episode/p07zt8qv?xto	10587	285	
☐	https://www.bbc.co.uk/iplayer/episode/p07zt8qv/sta	10878	300	
☐	https://www.bbc.co.uk/iplayer/episode/p07zt8qv/sta	11213	92	
☐	https://traffic.outbrain.com/network/redir?p=tYsY5u	11311	300	
☐	http://bbc.com/	12272	16	

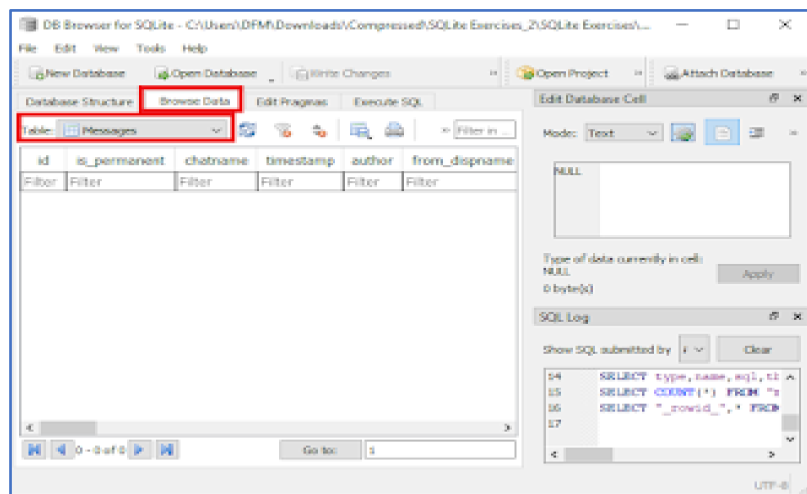
Unlocated Space (Carving)   (Belkasoft SQLite Viewer)

Important SQLite Forensics Note

SQLite Recovery လုပ်မယ်ဆိုရင် Storage ကို Write Protect လုပ်ရပါတယ်။ သာမန် Database Browser / Viewer နဲ့ ဖွင့်ရင် Commit မလုပ်ရသေးတဲ့ Journal File , WAL File တွေက Commit ဖြစ်ပြီး Data ပျောက်တတ်ပါတယ်။

Journal File, WAL File, Free List Pages တိုင်း Recovery မရပါဘူး။ Application Developer နဲ့ Vendor က SQLite Database ထဲမှာ သတ်မှတ် ရွေးချယ်တဲ့ Setting တွေပေါ်မှာလဲ မူတည်ပါတယ်။

SQLite Database အတွက် သီးသန့်ထုတ်ထားတဲ့ Recovery Tools နဲ့သာ Journal File , WAL File, Free List Pages, Unlocated Space တွေကို Recovery ပြုလုပ်လို့ရပါတယ်။



Open SQLite Database With DB Browser

SQLite Data Base ထဲမှာရှိတဲ့ Message Table ကို DB Browser နဲ့ဖွင့်ကြည့်ထားတာ ဖြစ်ပါတယ်။ Free List , Journal, WAL File တွေကို မတွေ့ရပါဘူး။

Properties
Tables
Accounts (1)
Alerts (0)
CallMembers (3)
Calls (3)
ChatMembers (10)
Chats (5)
ContactGroups (12)
Contacts (3)
Conversations (9)
DbMeta (4)
LegacyMessages (0)
Messages (53)
Participants (18)
SMSes (0)

Data | Structure

Record type	id [Primary key]	is_permanent	chatname	timestamp	author	from_dispname
Freelist	140	1	#belkasofttest/$+790!	1266832606	+79052045315	+79052045315
Freelist	138	1	#belkasofttest/$+790!	1266832594	belkasofttest	BelkaSoftTest
Freelist	109	1	#belkasofttest3/$belka	1266832570	belkasofttest3	belkasofttest3
Freelist	108	1	#belkasofttest3/$belka	1266832558	belkasofttest3	belkasofttest3
Freelist	105	1	#belkasofttest3/$belka	1266832551	belkasofttest3	belkasofttest3
Freelist	103	1	#belkasofttest3/$belka	1266832533	belkasofttest	BelkaSoftTest
Freelist	101	1	#belkasofttest3/$belka	1266832521	belkasofttest	BelkaSoftTest
Freelist	100	1	#belkasofttest3/$belka	1266832515	belkasofttest3	belkasofttest3
Freelist	99	1	#belkasofttest3/$belka	1266832511	belkasofttest	BelkaSoftTest
Freelist	98	1	#belkasofttest3/$belka	1266832506	belkasofttest3	belkasofttest3
Freelist	96	1	#belkasofttest3/$belka	1266832496	belkasofttest3	belkasofttest3

Recovery အတွက် (Belkasoft SQLite Viewer) နဲ့ဖွင့်ကြည့်ထားတာဖြစ်ပါတယ်။

REFERENCE - SQLite Forensics Training [(Belkasoft)]